Ēriks Dobelis, BITI

Interneta lietojumu (un ne tikai) drošības jaunumi 2012. gadā

Globālās informācijas drošības tendences

- 2012 Data Breach Investigations Report:
  - Kopējais pētījumā iekļauto incidentu zaudējumu novērtējums 174 miljoni USD
  - Būtiski pieaug ārējo uzbrukumu un krīt iekšējo lietotāju draudu (t.sk privilēģiju eskalācijas gadījumu) īpatsvars
  - Būtiski pieaug politiski vai tml. motivēto uzbrukumu skaits
  - Krītās sociālo metožu lietošanas īpatsvars
  - Stabili turpina attīstīties automatizētie uzbrukumi vāji aizsargātajiem tīkla resursiem

BITI

Globālās informācijas drošības tendences

- 2012 Data Breach Investigations Report:
  - 85% veiksmīgo uzbrukumu netika atklāti pirmajās 2 nedēļās
  - 97% veiksmīgo uzbrukumu varēja tikt atvairīti ar vienkāršām vai vidēji sarežģītām kontrolēm
  - 96% veiksmīgo uzbrukumu nebija īpaši sarežģīti
  - 92% veiksmīgo uzbrukumu atklāja trešā puse

BITI

Hakeru tendences

- Joprojām pieaug interese par SQL injekcijām
- Tipiskie uzbrukumi ir automatizēti un parasti ilgst 8-10 minūtes
- Uzbrukumi sociālo tīklu lietotājiem izspiešanas nolūkā

- Pēc Imperva Hacker Intelligence Initiative, Monthly Trend Report #3 un #13 datiem

BITI

Nomainiet paroles ☺ (atkal)

- Amazon Zappos 24 miljoni lietotāju/paroļu
- 12 miljoni Apple ID u.c. info nozagti no FIB aģenta datora, daļa datu publicēti
- LinkedIn 6.5 miljoni lietotāju/paroļu hešu
- Yahoo 137-400 tūkstoši lietotāju/paroļu (SQL injekcija)
- Blizzard Battle.net ? paroļu hešu (SQL injekcija)
- IEEE 100 tūkstoši biedru lietotāji/paroles

BITI

APT (Advanced Persistent Threat)

- Ilgtermiņa, mērķēti, sarežģīti uzbrukumi, bieži ar valdību atbalstu
- Ļoti grūti pamanāmi
- 2010. gada uzbrukumi Stuxnet, RSA kā pirmie līdzīga mēroga gadījumi, 2011. gadā – Duqu
- Flame – audio ierakstīšana, ekrāna kopijas, klaviatūras aktivitātes
- Wiper – veidots masveidīgai datu iznīcināšanai
- Gauss – vīruss mērķēts uz dažu Libānas banku, CitiBank un PayPal lietotāju darbību reģistrēšanu

BITI

SSRF/XXE uzbrukumi

- Uzbrukumi iekšējām sistēmām, nosūtot pieprasījumus ārējām sistēmām
- Iekšējās sistēmas bieži ir vājāk aizsargātas, bez pēdējiem jauninājumiem
- Ārējās sistēmās ne vienmēr ir nofiltrēts viss, kas var radīt ietekmi
- Piemēram:
  - interneta veikals, kas integrēts ar ERP
  - internetbanka, kas ļauj ielādēt XML?

BITI

XXE piemērs

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE manstips [
    <!ELEMENT manstips ANY >
    <!ENTITY datums SYSTEM
    “gopher://172.16.0.1:3300/123456789" >
    ]>
<manstips>&datums</manstips>
```

BITI

Interneta lietojumu 'skrāpēšana'

- Piemēram, Facebook incidents (2012. gada oktobrī)
- Mērķis – masveidā izgūt publicētus datus no interneta lietojuma ar vai bez pakalpojuma sniedzēja piekrišanas
- Agrāk plaši izmantotie rīki nespēja tikt galā ar Javascript bāzētām lapām, šobrīd - spēj

BITI

Interneta lietojumu 'skrāpēšana'

- Plaši pazīstami piemēri – internetveikalu cenu, aviobiļešu cenu, valūtu kursu u.c. salīdzināšanas lapas
- Datu meklēšana ģenerējot personas kodus, telefona numurus automašīnu reģistrācijas numurus un tml.
- Riski:
  - Apkopotas un regulāri atjaunotas informācijas publicēšana var būt nevēlama
  - Noslodzes radītas veiktspējas problēmas
  - Pieprasījumu apstrādes izmaksas

BITI

Interneta lietojumu 'skrāpēšana'

- Aizsardzība:
  - Tranzakcijas pret pieprasījumu skaitu
  - Navigācijas un pieprasījumu datu analīze
  - CAPTCHA (šobrīd drošākā metode, bet apgrūtinājums lietotājam)

BITI

Uzbrukums PHP gadījumskaitļiem

- Izplatīta nedrošu funkciju izmantošana gadījumskaitļu ģenerēšanai
- Līdzīgi uzbrukumi iespējami pret citām populārām interneta lietojumu valodām/ietvariem
- Dažām testētajām sistēmām uzminēts sesijas id vidēji pēc dažiem tūkstošiem pieprasījumu
- Pilns raksts:

https://media.blackhat.com/bh-us-12/Briefings/Argyros/BH_US_12_Argyros_PRNG_WP.pdf

BITI

Integrētie uzbrukumi

- Uzbrukumi, kas ietver vairākus soļus no tipiskām bieži sastopamām ievainojamībām
- Scenārija piemērs:
  - Lietotājs apmeklē uzbrucēja mājas lapu
  - Izpildās Javascript skaneris, kas meklē populārus maršrutizētāju modeļus
  - Autentifikācija ar noklusējuma/uzminētu paroli
  - Modificētas OS programmatūras augšupielāde maršrutizētājā
  - Pilna kontrole

BITI

Integrētie uzbrukumi

- «Pierunājam» lietotāju aiziet uz specifisku mājas lapu ar kodu:

  <iframe onload="foundactivehost(this);"
  src="http://192.168.1.1:80"></iframe>
- Šāds pieprasījums izpilda nodoto Javascript funkciju, ja tiek atrasts serveris norādītajā adresē
- Protams, varam ģenerēt plašākus IP adrešu diapazonus, kas ir tipiski iekšējiem tīkliem

- Zināt, ko dara ?

BITI

Integrētie uzbrukumi

- Kas ir nepieciešams, lai tas izdotos?
  - Lietotājs aiziet uz konkrētu lapu (viegli)
  - Tiek uzminēts iekšējo adrešu diapazons (192.168.1.0/24 uzminēt ir viegli)
  - Tiek izmantots populārs maršrutizētājs (dažus īpaši populārus modeļus var sastapt no mājas lietotājiem līdz lielām korporācijām)
  - Maršrutizētāja parole ir viegli uzminama (ja ir ilūzija, ka iekšējais tīkls ir aizsargāts – viegli)
- Vairāku bieži sastopamu lietu sakritība

BITI

…bet LV nekas nav mainījies:

joprojām lielākai daļai interneta lietojumu tikai viena līmeņa aizsardzība

kas ir interneta lietojumu ugunsmūri (WAF) zin tikai izredzētie

un par SQL injekcijām izstrādātājiem universitātē nemāca

Jautājumi?

Ēriks Dobelis
Twitter @eriksdobelis
www.biti.lv